

# Cookies and Sessions

## Maintaining State in HTTP



open.michigan

Unless otherwise noted, the content of this course material is licensed under a Creative Commons Attribution 3.0 License.

<http://creativecommons.org/licenses/by/3.0/>.

Copyright 2009, Charles Severance

# High Level Summary

- The web is “stateless” - the browser does not maintain a connection to the server while you are looking at a page. You may never come back to the same server - or it may be a long time - or it may be one second later
- So we need a way for servers to know “which browser is this?”
  - In the browser state is stored in “Cookies”
  - In the server state is stored in “Sessions”

## Welcome to SI539

- About
- Contact
- Pictures
- Membership
- Chat
- Application

### Please Log In

Required Information

Enter your E-Mail:

Enter your Password:

If you have lost your password,  
membership@si539.com to have

## UNIVERSITY OF MICHIGAN WEBLOGIN

### AUTHENTICATION REQUIRED::

You are connecting to a U-M website that requires authentication. Please enter your Login ID (username or Friend ID) and password to continue.

#### Need a Login ID?

If you don't have a Login ID, you can [create one now](#).

Login ID

Password

[Forgot your password?](#)

[Login Help](#)

By using this service you agree to adhere to [U-M computing policies and guidelines](#).

Some Web sites always seem to want to know who you are!


# twitter

Home Find & Follow Public Timeline Settings Help Sign out

What are you doing?

140

Hi, [your profile](#)

 drchuck

update

Recent Replies Archive



**dkeats** Spending the morning with the eLearning team innovation, and participation in a community of practice Energizing. 3 minutes ago from web ☆ ↻



**drchuck** Working on lecture slides – talking about cool sessions. 5 minutes ago from web ☆ ↻



**Matth** Ordered Urban Fortunes from Amazon because saying it said things I wasn't at all agreeing with. Right. ago from twitterrific ☆ ↻



**microcline** Back from walking the dogs. Cleaned them can, but they don't get to share the futon tonight. 31 m from web ☆ ↻

## flickr

Home You Organize Contacts Groups Explore

Signed in as dr-chuck (1 new)

Search everyone's photos



## Ni hao dr-chuck!

Now you know how to greet people in Mandarin!

- You have 1 new message.
- [Find your friends](#)

### Flickr News

31 Mar 08 - Flickr is more fun with friends, but it is a big busy place, and sometimes it can be hard to find the people you know. The new Find Your... [read more news](#)

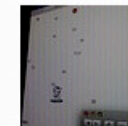
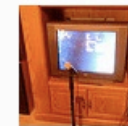
» [Flickr Blog](#) Great photos & latest news, daily!

ADVERTISEMENT



» [Upload Photos](#) (Or, look at our uploading [tools...](#))

» [Your Photos](#) ([Recent activity](#) / [Comments you've made](#))



» [Photos from your Contacts](#)



From [Lance70](#)



From [Lance70](#)



From [Lance70](#)



From [Lance70](#)

Other Web sites always seem to know who you are!

Browser

Click Draw



You watch the YouTube video  
for an 30 seconds

Whole  
Page

GET

Click Draw

Whole  
Page

GET

Server

How you see YouTube...

Browser

Click

Draw

Click

Draw

Whole  
Page

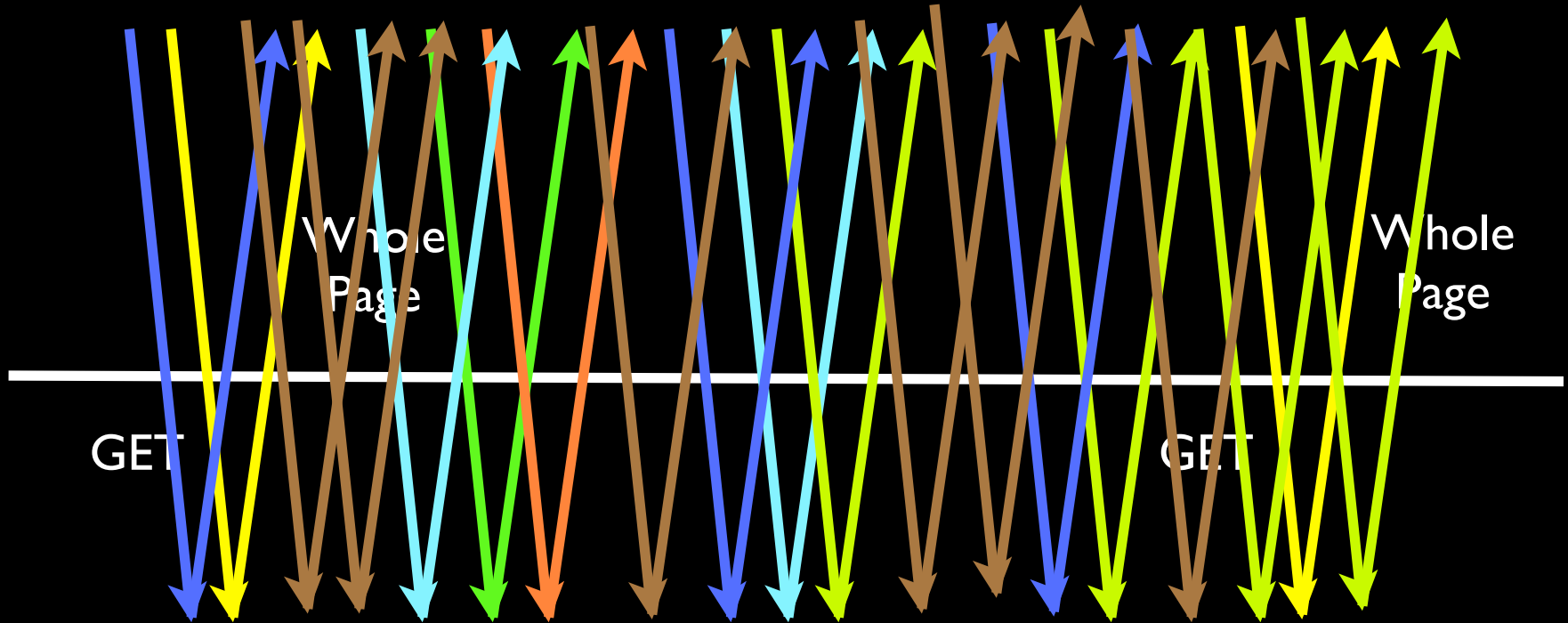
Whole  
Page

GET

GET

Server

How YouTube sees you...



# Multi-User

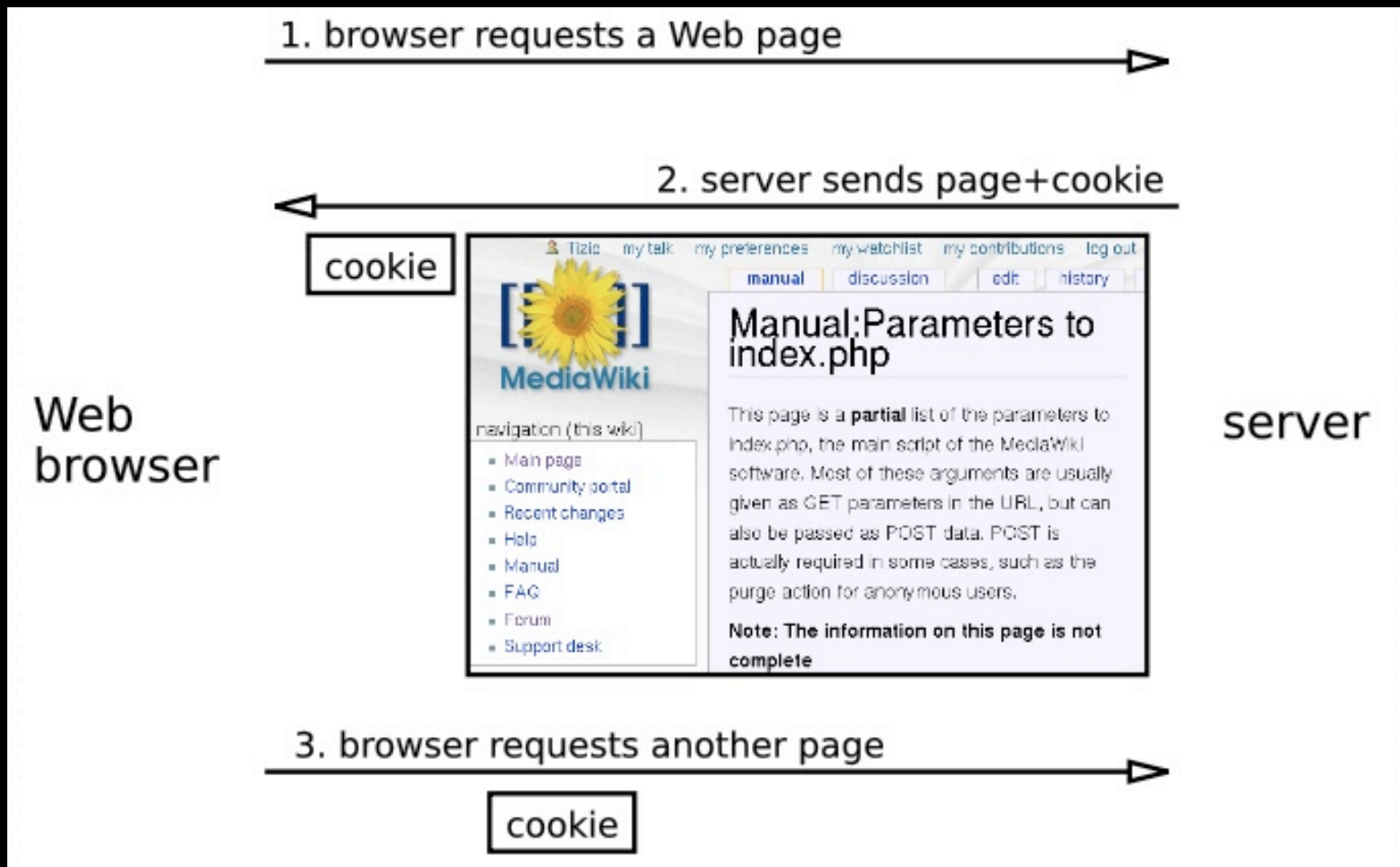
- When a server is interacting with many different browsers at the same time, the server needs to know \*which\* browser a particular request came from
- Request / Response initially was stateless - all browsers looked identical - this was really really bad and did not last very long at all.



# Web Cookies to the Rescue

*Technically, cookies are arbitrary pieces of data chosen by the Web server and sent to the browser. The browser returns them unchanged to the server, introducing a state (memory of previous events) into otherwise stateless HTTP transactions. Without cookies, each retrieval of a Web page or component of a Web page is an isolated event, mostly unrelated to all other views of the pages of the same site.*

[http://en.wikipedia.org/wiki/HTTP\\_cookie](http://en.wikipedia.org/wiki/HTTP_cookie)



[http://en.wikipedia.org/wiki/HTTP\\_cookie](http://en.wikipedia.org/wiki/HTTP_cookie)

# Cookies In the Browser

- Cookies are marked as to the web addresses they come from - the browser only sends back cookies that were originally set by the same web server
- Cookies have an expiration date - some last for years - others are short-term and go away as soon as the browser is closed

# Playing with Cookies

- Firefox Developer Plugin has a set of cookie features
- Other browsers have a way to view or change cookies

## Welcome to SI539

- **About**
- **Contact**
- **Pictures**
- **Membership**
- **Chat**
- **Application**
- **Logout**

### Welcome to the SI539 Sakai

Here are two quotes from Ghandi that look like they reach the same conclusion.

Power is of two kinds. One is obtained by the use of force, the other by acts of love. Power based on force is effective and permanent then the other.

I hope to demonstrate that the real source of authority by a few, but by the acquisition of authority, when abused.

Cookie Information - http://localhost:3000/One

Sakai dr-chuck.com NWA Chuck's Media iPhone Navigation I3k CT SI 182 Sakai Based Service : ...

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize

Ass

Disable Cookies

Clear Session Cookies

Delete Domain Cookies

Delete Path Cookies

View Cookie Information

Add Cookie...

Collaps

http://localhost:3000/One

1 cookie

NAME	_assn6_session_id
VALUE	fa3e49c915aad8bd9af1f768b8081aa6
HOST	localhost
PATH	/
SECURE	No
EXPIRES	At End Of Session

Done

# Cookies

- Identifying Individual Users
- The Web is “stateless”
- How do we make the web seem not to be stateless

Request Response Again!

# HTTP Request / Response Cycle

(Review)

Web Server

HTTP  
Request

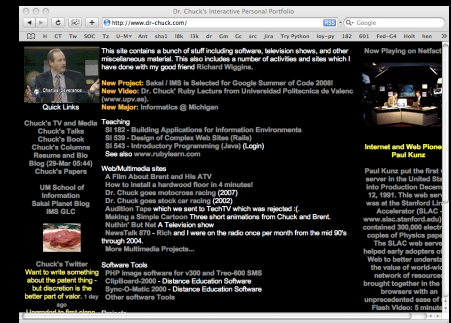
HTTP  
Response

Browser

Hello there my name is Chuck  
Go ahead and click on [here](#).

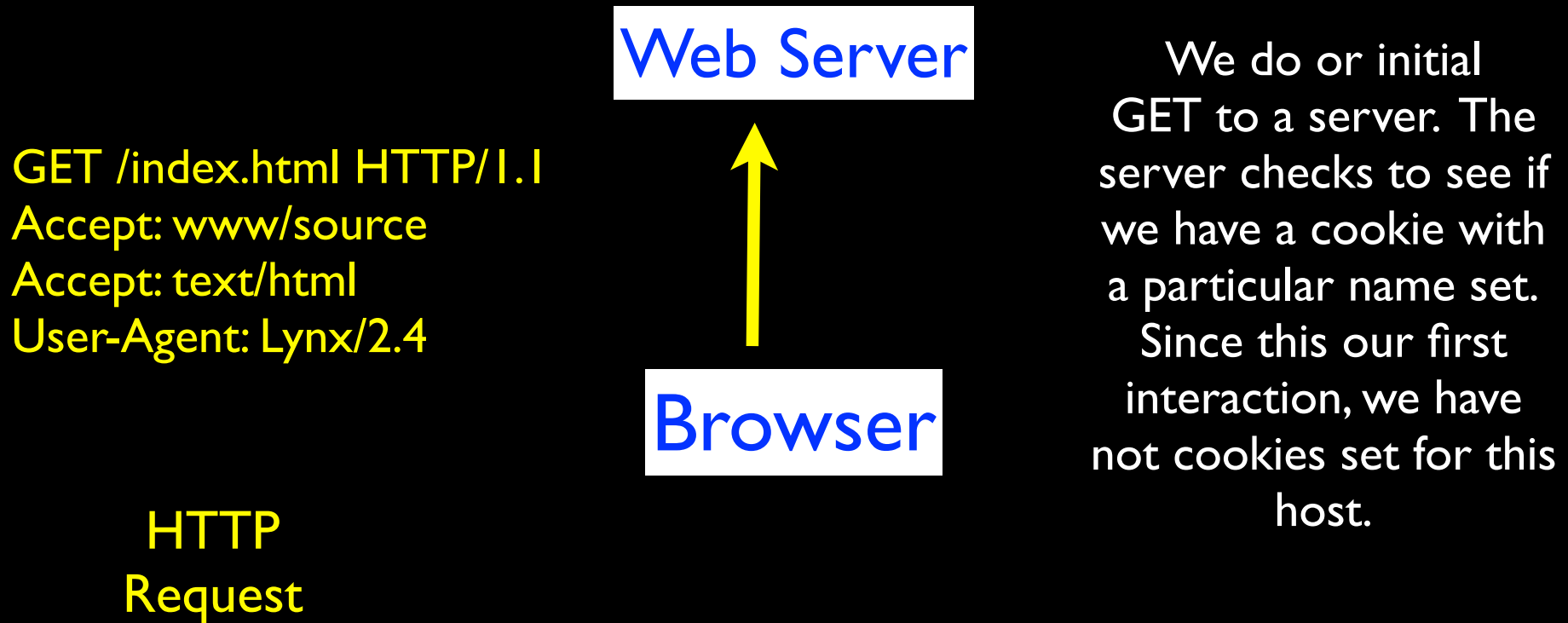
Internet Explorer,  
FireFox, Safari, etc.

[http://www.oreilly.com/openbook/cgi/ch04\\_02.html](http://www.oreilly.com/openbook/cgi/ch04_02.html)

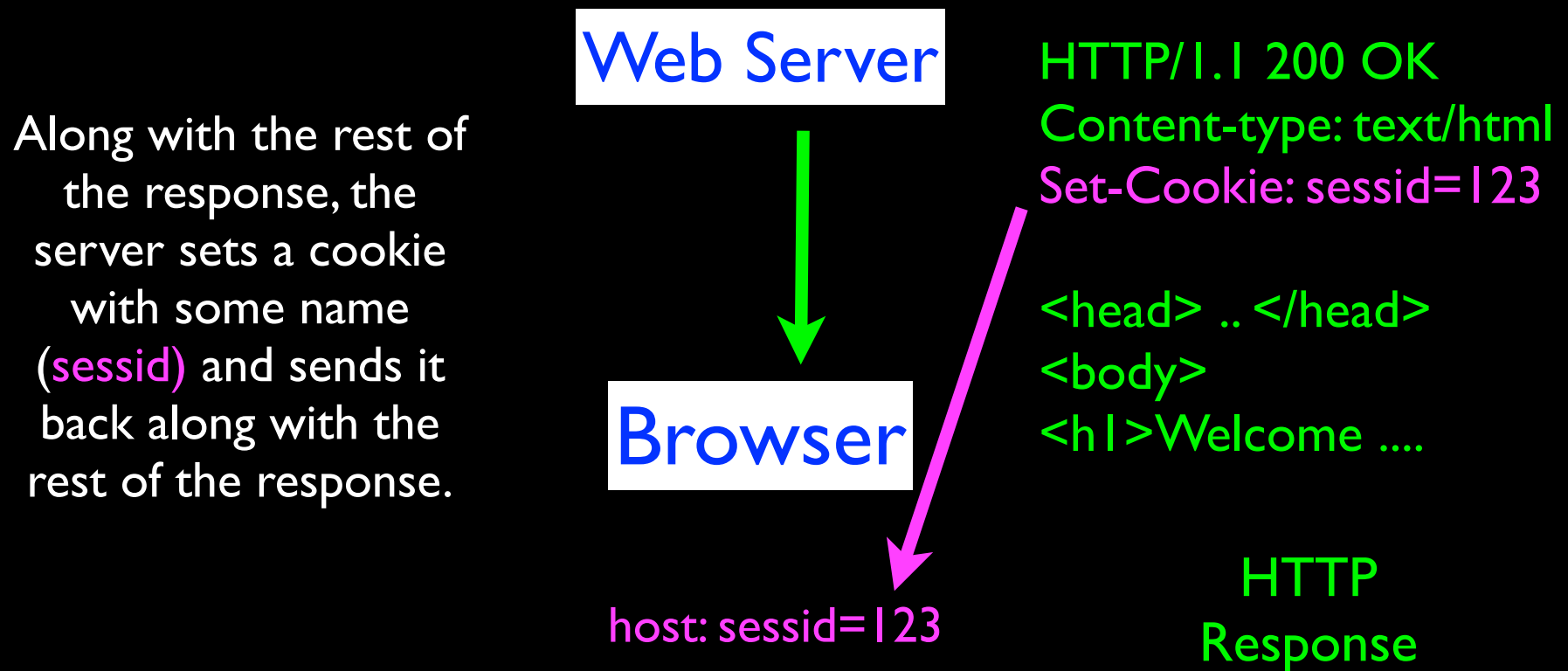




# HTTP Request / Response Cycle



# HTTP Request / Response Cycle



[http://www.oreilly.com/openbook/cgi/ch04\\_02.html](http://www.oreilly.com/openbook/cgi/ch04_02.html)

# HTTP Request / Response Cycle

GET /index.html HTTP/1.1  
Accept: www/source  
Accept: text/html  
Cookie: sessid=123  
User-Agent: Lynx/2.4

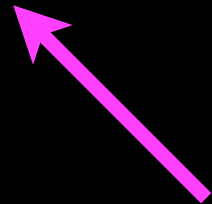
HTTP  
Request

Web Server



Browser

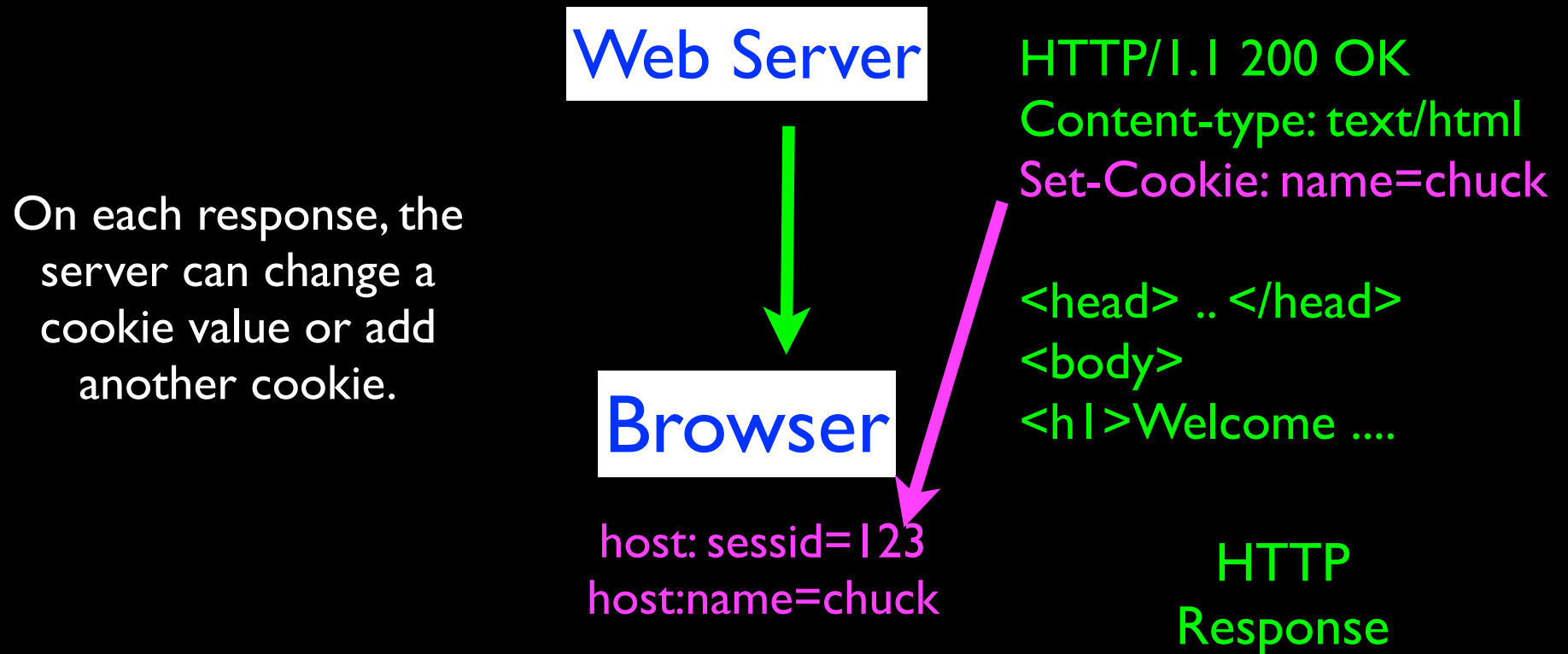
host: sessid=123



From that point forward, each time we send a GET or POST to the server, we include any cookies which were set by that host.

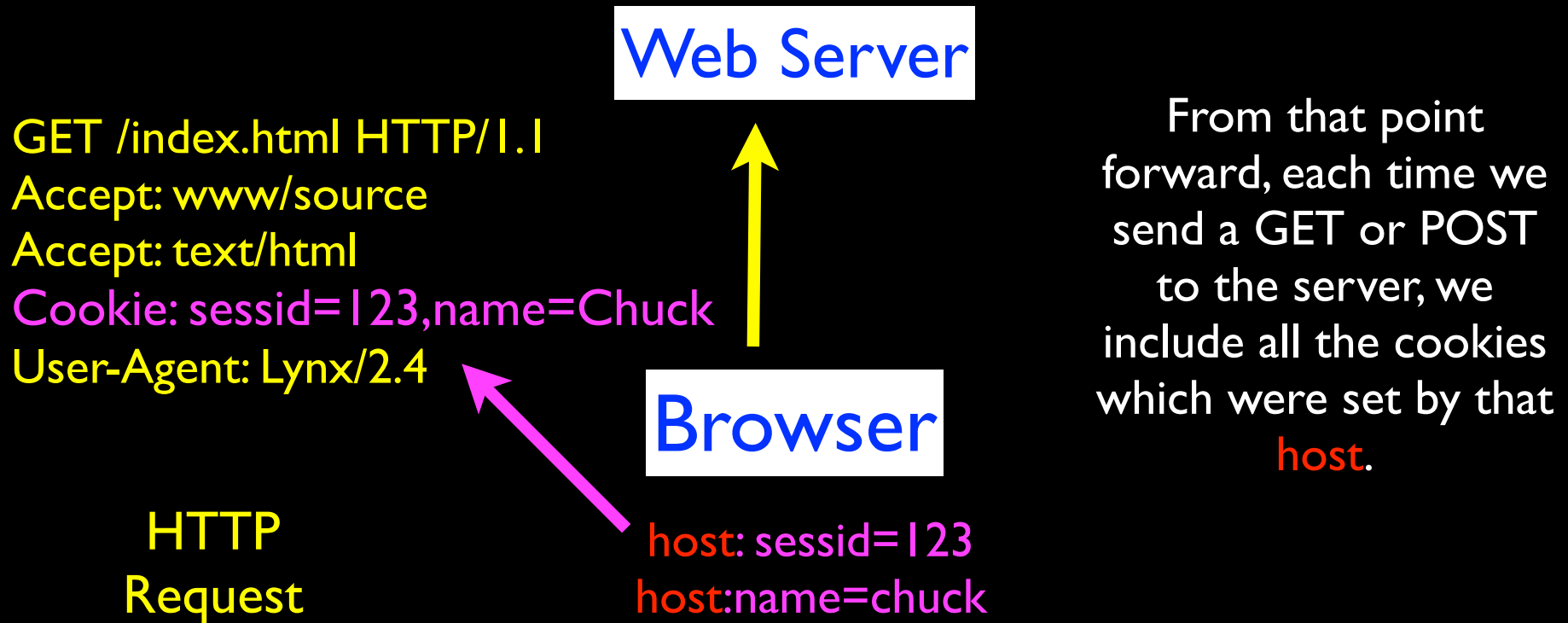
[http://www.oreilly.com/openbook/cgi/ch04\\_02.html](http://www.oreilly.com/openbook/cgi/ch04_02.html)

# HTTP Request / Response Cycle



[http://www.oreilly.com/openbook/cgi/ch04\\_02.html](http://www.oreilly.com/openbook/cgi/ch04_02.html)

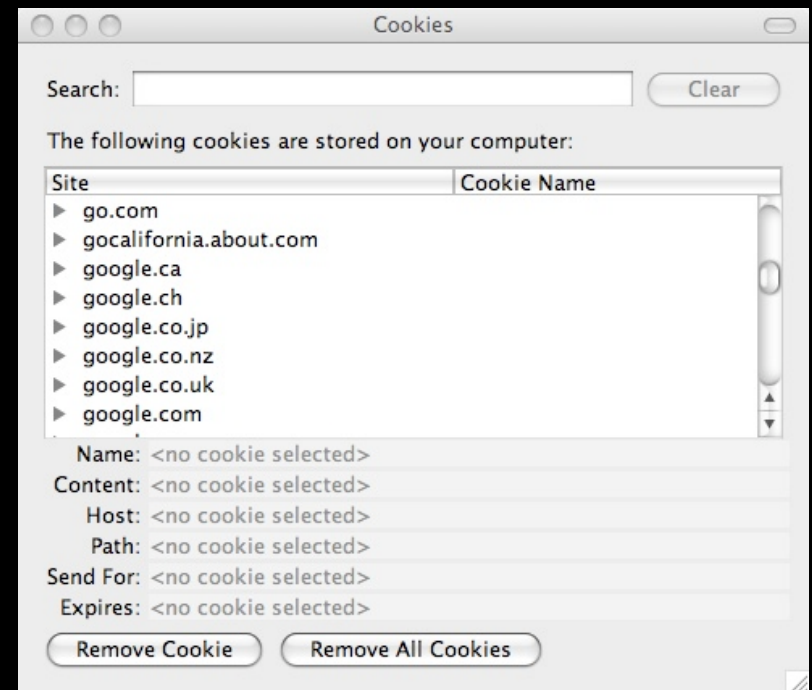
# HTTP Request / Response Cycle



[http://www.oreilly.com/openbook/cgi/ch04\\_02.html](http://www.oreilly.com/openbook/cgi/ch04_02.html)

# Security

- We only send cookies back to the host that originally set the cookie
- The browser has \*lots\* of cookies for lots of hosts
- To see all Cookies: Firefox -> Preferences -> Privacy -> Show Cookies



Cookie Information - http://www.dr-chuck.com/

Sakai dr-chuck.com NWA Chuck's Media iPhone Navigation I3k CT SI 182 Sakai Based Service : ... portal

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools

Dr. Chuck's Interactive Person... Cookie Information - http://ww...

NAME	__utmb
VALUE	140904167
HOST	.dr-chuck.com
PATH	/
SECURE	No
EXPIRES	Wed, 24 Sep 2008 10:28:02 GMT

Edit Cookie

Delete Cookie

NAME	__utmc
VALUE	140904167
HOST	.dr-chuck.com
PATH	/
SECURE	No
EXPIRES	At End Of Session

Done

The Firefox Web Developer Plugin Shows Cookies for the Current Host.

# Two Kinds of Cookies

- Two kinds of cookie
  - Long-lived - who you are - account name last access time - you can close and reopen your browser and it is still there
  - Temporary - used to identify your session - it goes away when you close the browser



Cookie Information - http://www.dr-chuck.com/

Sakai dr-chuck.com NWA Chuck's Media iPhone Navigation I3k CT SI 182 Sakai Based Service : ... portal

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools

Dr. Chuck's Interactive Person... Cookie Information - http://ww...

NAME	__utmb
VALUE	140904167
HOST	.dr-chuck.com
PATH	/
SECURE	No
EXPIRES	Wed, 24 Sep 2008 10:28:02 GMT

[Edit Cookie](#)

[Delete Cookie](#)

NAME	__utmc
VALUE	140904167
HOST	.dr-chuck.com
PATH	/
SECURE	No
EXPIRES	At End Of Session

Done

# Using Cookies to Support Sessions and Login / Logout

## Welcome to SI539

- About
- Contact
- Pictures
- Membership
- Chat
- Application

### Please Log In

Required Information

Enter your E-Mail:

Enter your Password:

If you have lost your password,  
membership@si539.com to have

## UNIVERSITY OF MICHIGAN WEBLOGIN

### AUTHENTICATION REQUIRED::

You are connecting to a U-M website that requires authentication. Please enter your Login ID (username or Friend ID) and password to continue.

#### Need a Login ID?

If you don't have a Login ID, you can [create one now](#).

Login ID

Password

[Forgot your password?](#)

[Login Help](#)

By using this service you agree to adhere to [U-M computing policies and guidelines](#).

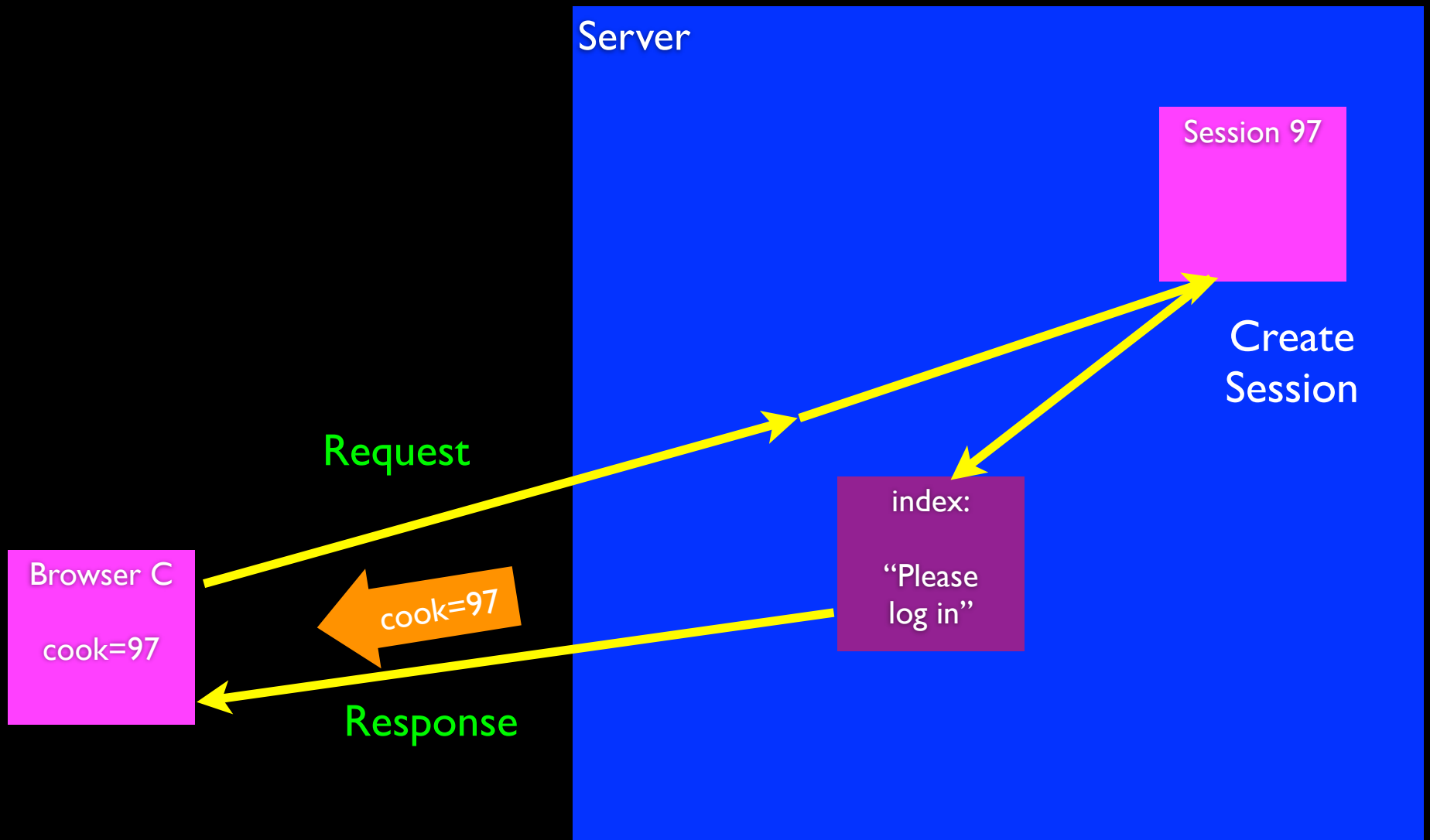
Some Web sites always seem to want to know who you are!

# In The Server - Sessions

- In most server applications, as soon as we meet a new browser - we create a session
- We set a session cookie to be stored in the browser which indicates the session id in use
- The creation and destruction of sessions is generally handled by a web framework or some utility code that we just use to manage the sessions

# Session Identifier

- A large, random number that we place in a browser cookie the first time we encounter a browser.
- This number is used to pick from the many sessions that the server has active at any one time.
- Server software stores data in the session which it wants to have from one request to another from the same browser.
- Shopping cart or login information is stored in the session in the server



# Typing

**Welcome to SI539**

- About
- Contact
- Pictures
- Membership
- Chat
- Application

**Please Log In**

Required Information

Enter your E-Mail:

Enter your Password:

If you have lost your password, please send an E-Mail to [membership@si539.com](mailto:membership@si539.com) to have your password reset.

Browser C

cook=97

## Server

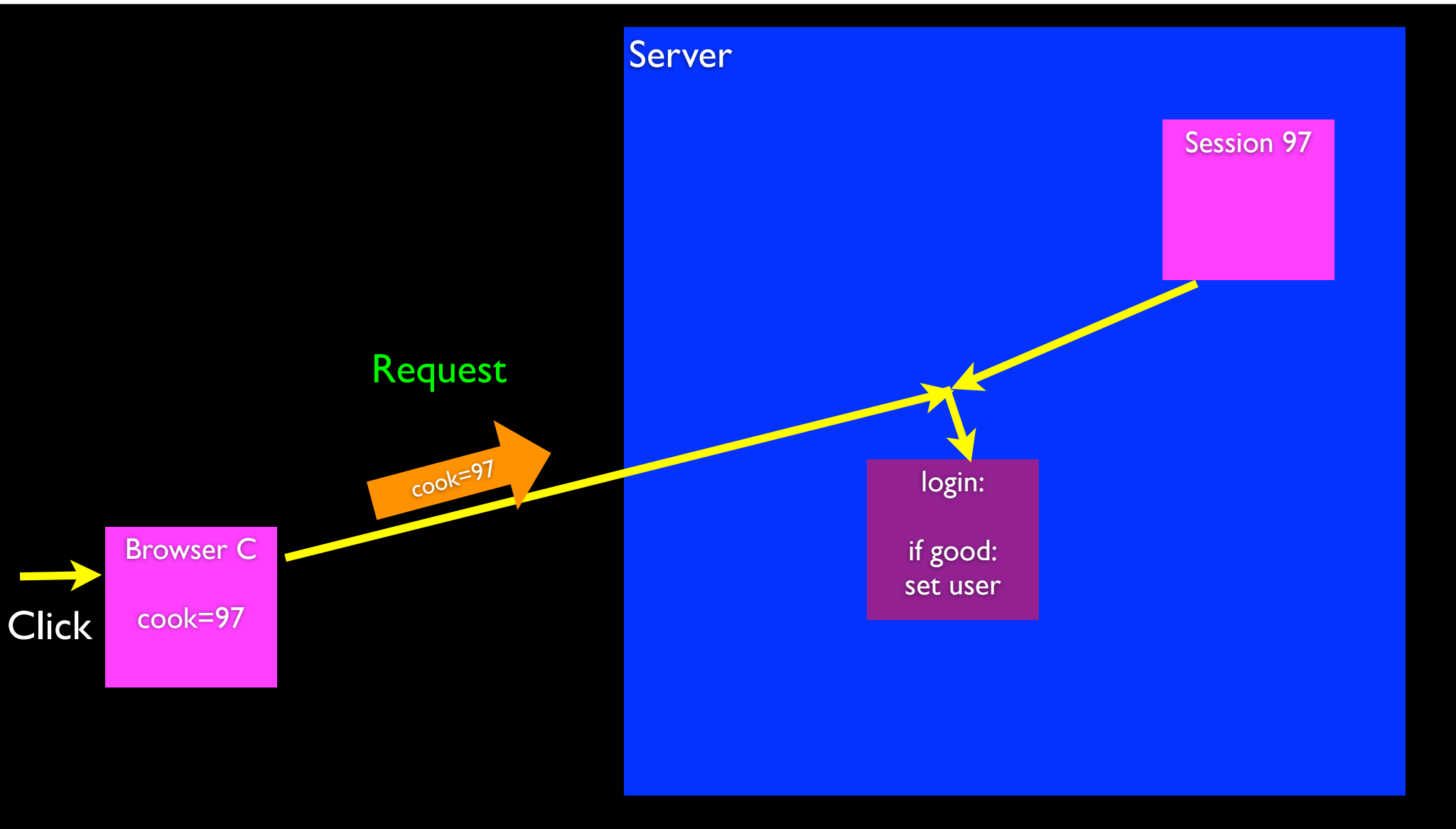
Session 97

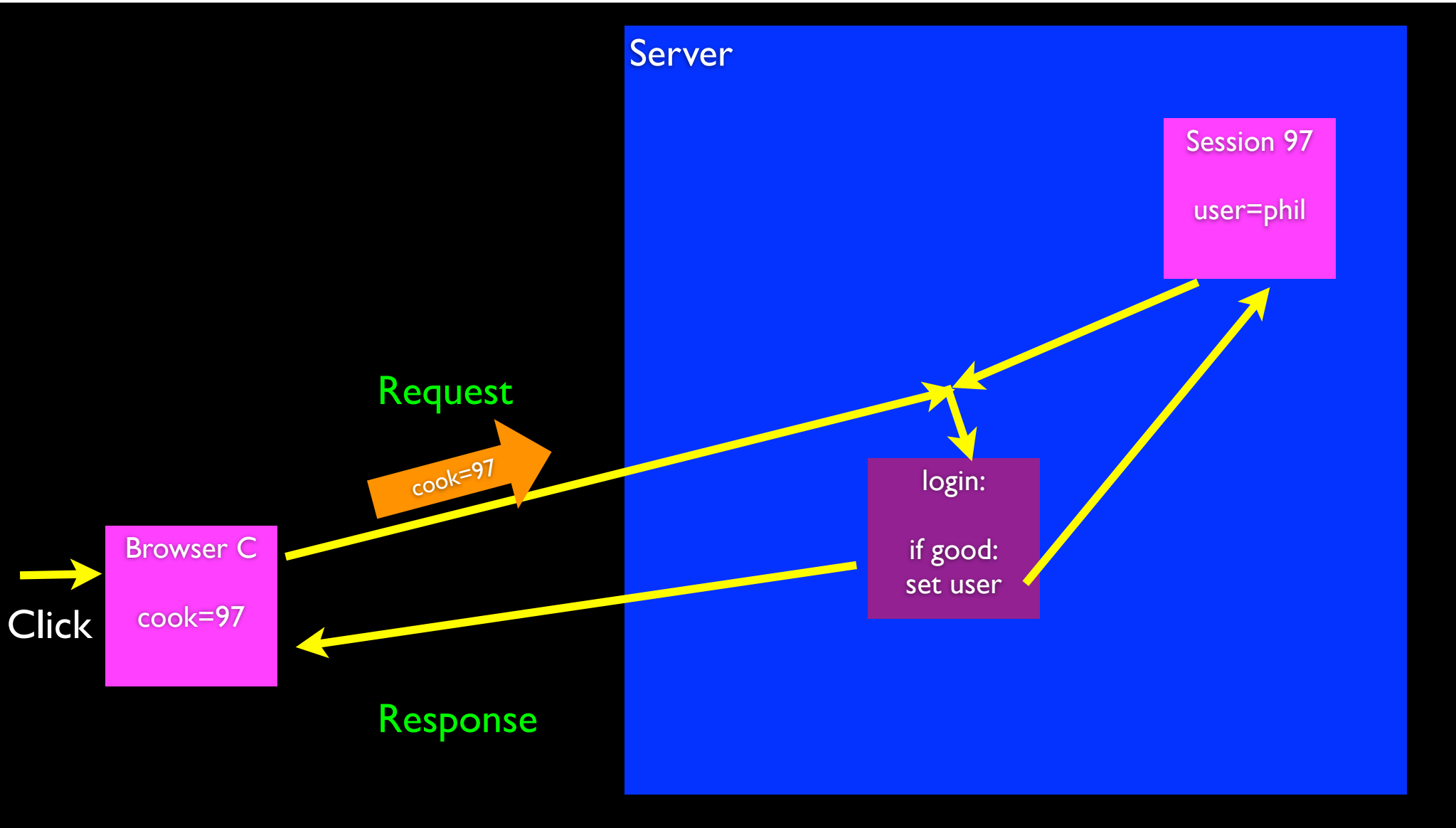
We now have a  
session established  
but are not yet  
logged in.

# Login / Logout

- Having a session is not the same as being logged in.
- Generally you have a session the instant you connect to a web site
- The Session ID cookie is set when the first page is delivered
- Login puts user information in the session (stored in the server)
- Logout removes user information from the session







Server

Session 97

user=phil

Browser C

cook=97

Using Sessions for Other Stuff

Browser A

cook=10

Browser B

cook=46

Server

Session 10

user=chuck  
bal=\$1000

Session 46

user=jan  
bal=\$400

Browser A

cook=10

Browser B

cook=46

Server

Session 10

user=chuck  
bal=\$1000

Session 46

user=jan  
bal=\$500

withdraw:

bal=bal-100

Click →

Browser A

cook=10

Browser B

cook=46

Server

Session 10

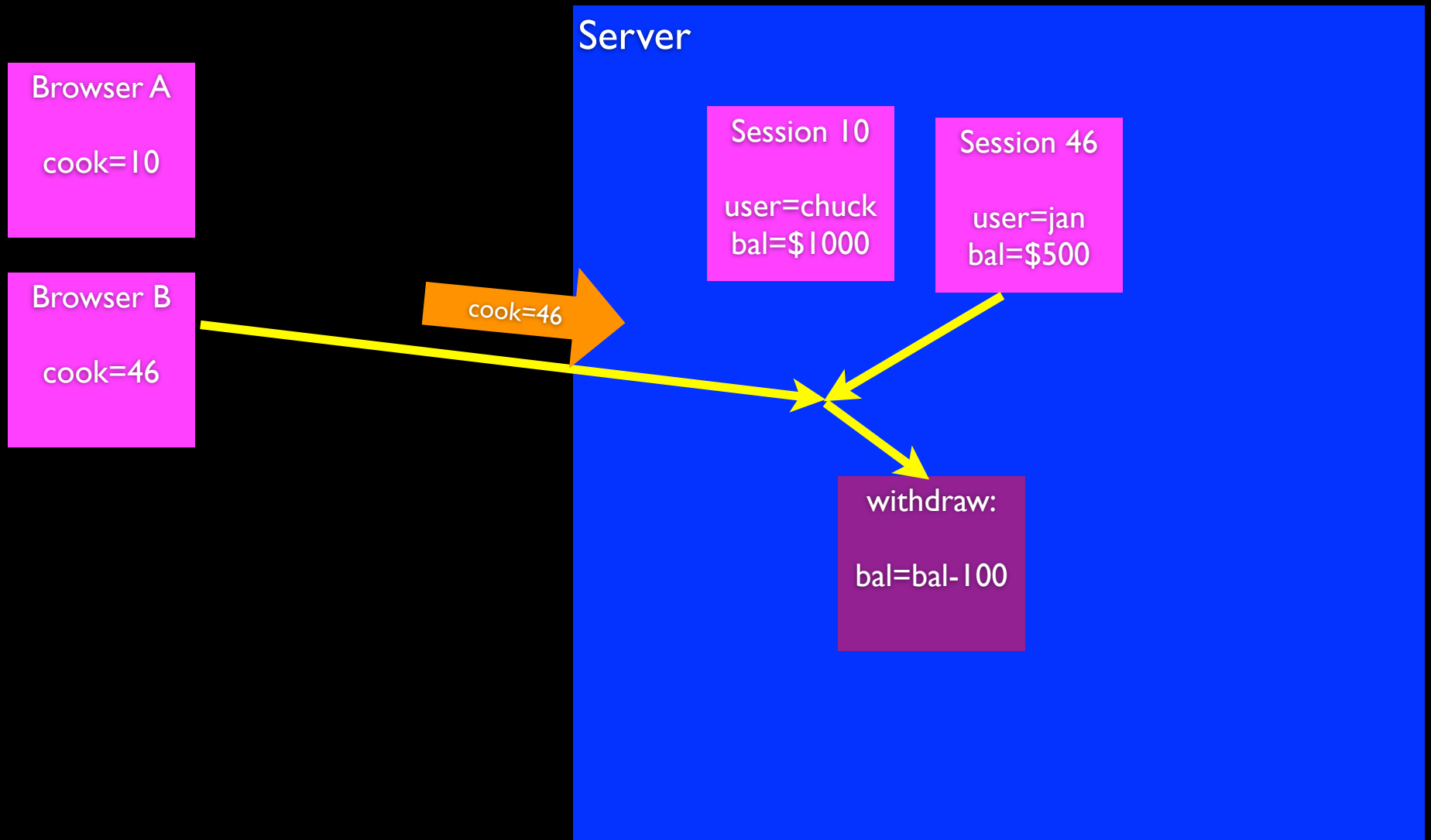
user=chuck  
bal=\$1000

Session 46

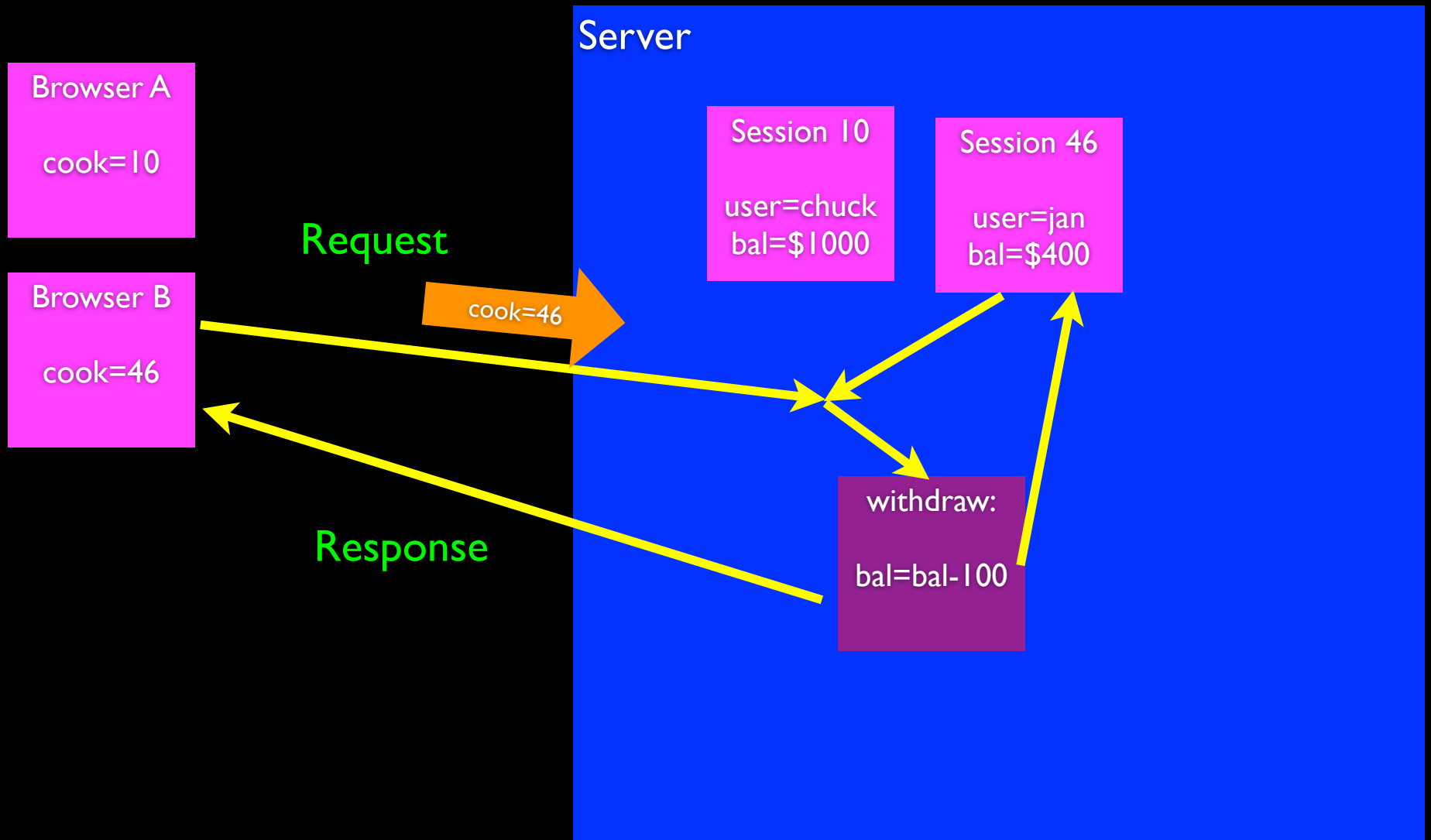
user=jan  
bal=\$500

withdraw:

bal=bal-100







Review...

# High Level Summary

- The web is “stateless” - the browser does not maintain a connection to the server while you are looking at a page. You may never come back to the same server - or it may be a long time - or it may be one second later
- So we need a way for servers to know “which browser is this?”
  - In the browser state is stored in “Cookies”
  - In the server state is stored in “Sessions”

Browser

Click Draw



You watch the YouTube video  
for an 30 seconds

Whole  
Page

GET

Click Draw

Whole  
Page

GET

Server

How you see YouTube...

# Browser

# Click

# Draw

# Whole Page

GET

Click

## Draw

# Whole Page

# GET

# Server

Browser

Click Draw

Click Draw

Whole  
Page

Whole  
Page

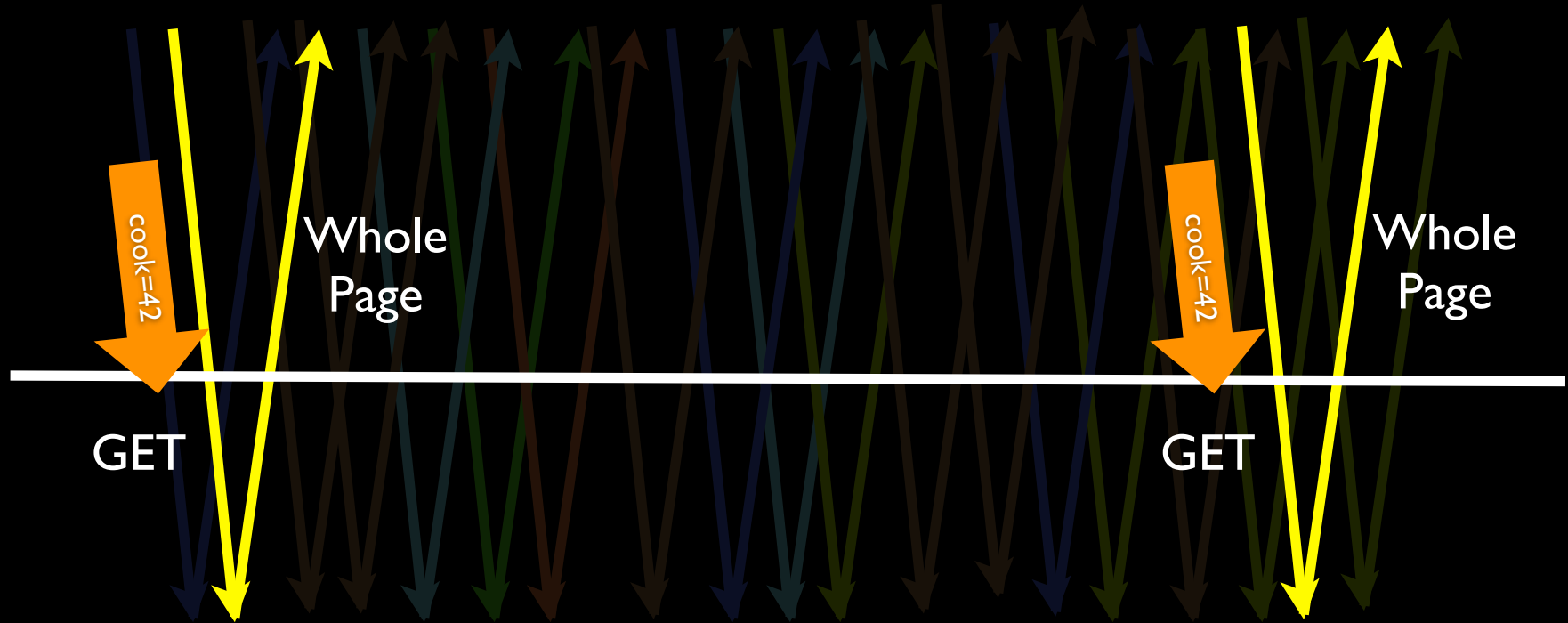
GET

GET

Server

Session 42

Session 42



# Cookie/Session Summary

- Cookies take the stateless web and allow servers to store small “breadcrumbs” in each browser.
- Session IDs are large random numbers stored in a cookie and used to maintain a session on the server for each of the browsers connecting to the server
- Server software stores sessions \*somewhere\* - each time a request comes back in, the right session is retrieved based on the cookie
- Server uses the session as a scratch space for little things